Department of the Army
Headquarters, United States Army
Training and Doctrine Command
Fort Monroe, Virginia 23651-5000

TRADOC Pamphlet 25-71

1 April 1997

Information Management: Automation

STANDARDS FOR ELECTRONIC STAFFING, PUBLISHING, AND ARCHIVING

Summary. This pamphlet describes the standards for automated systems based on an Open Systems philosophy supported by the Army Technical Architecture, version 4.0. It addresses standards for automating the staffing, publishing, and archiving of training and doctrinal products.

Applicability. This pamphlet applies to HQ TRADOC, TRADOC installations, schools, and activities that publish training and doctrinal products. It is provided as a guide to action officers who process training and doctrinal products.

Suggested improvements. The proponent of this pamphlet is the Deputy Chief of Staff for Information Management (DCSIM). Users should send comments and suggested improvements, by electronic mail, in the format of DA Form 2028 (Recommended Changes to Publications and Blank Forms), through channels to Commander, TRADOC, ATTN: ATIM-I, 183 McNair Drive, Fort Monroe, VA 23651-5000. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program (AIEP) Proposal). Electronic mail address: atimi@emh10.monroe.army.mil.

Availability. This publication is also available on the TRADOC Homepage at http://www-tradoc.army.mil.

Contents

Chapter 1
Introduction

1-1. Purpose. As TRADOC becomes more dependent on information technology in its transition to FORCE XXI, information systems must be able to connect and exchange data. This can be achieved by using commercially available software and compatible operating systems that enable properly engineered components to be used across a wide range of systems with minimum changes. These systems interoperate with other components on local and remote systems. Moreover, this pamphlet covers the processes for the digital dissemination of training and doctrine products within TRADOC.

1-2. References. Required and related publications and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations and terms. Abbreviations and special terms used in this pamphlet are explained in the glossary.

Chapter 2
Staffing

2-1. General requirements for an electronic doctrine and training development system. The electronic training development and doctrine system provides synchronization and sharing of information.

a. Training products are developed IAW TRADOC Reg 350-70.

b. As a minimum, the system must be capable of digitally accomplishing the tasks that are currently handled during the doctrine phase, described below:

(1) Assessment. Identify requirements to revise or develop a doctrine product.

(2) Planning.

(a) Consolidate/reduce redundancies or excesses.

(b) Review/modify doctrine publication hierarchy.

(c) Prioritize requirements.

(d) Identify start date.

(e) Prepare Program Directive (PD).

(f) Identify and assign resources.

(g) Establish management plan.

(3) Development and preparation.

(a) Confirm PD.

(b) Establish milestones.

(c) Conduct research.

(d) Apply TRADOC Reg 25-30 standard.

(e) Staff drafts.

(f) Integrate draft.

(g) Process for approval.

(4) Printing and distribution.

(a) Prepare/submit IAW TRADOC Reg 25-30.

(b) Disseminate.

(5) Implementation and evaluation.

(a) Validate fielded doctrine.

(b) Coordinate with CALL and JCLL.

2-2. Electronic staffing system components. The system must have a means to access the current inventory of products. Within this environment, doctrine and training developers must access any product, conduct queries or establish information linkages, analyze data, conduct coordination with other agencies, effect necessary changes, and prepare products for final approval. This staffing system provides a refined method for synchronizing doctrine and training information. Ultimately, an electronic system for staffing doctrine and training products allows digital transmission rather than paper-based distribution. The following features should be resident in or a component of the electronic system:

a. A database of doctrine and training products:

(1) Field manuals.

(2) Selected joint publications and other Service manuals.

(3) Training products/materials.

(4) Training circulars.

(5) Army regulations.

(6) Selected Army and TRADOC administrative publications.

b. A program for developers with the following capabilities:

(1) Able to access the product database.

(2) Perform queries, searches, and other database functions.

(3) Possess features for editing and preparing draft products.

(4) Provide a mechanism for staff coordination which includes:

(a) Method for sending a draft document to single or multiple addressees for eview/comment.

(b) Means of alerting addressees of incoming mail.

(c) Method for addressees to edit and/or comment on drafts.

(d) Capability to return addressee edited drafts/ comments to the originator which can be easily incorporated into a master draft.

(e) Capability for addressees to access all comments and edited draft input at each level within the chain of command—a collaborative working environment.

(f) Capability for developers to maintain visibility of the approval process for any product.

(5) Provide automatic formatting capabilities for screen and print.

(6) Provide management functions and tools for—

(a) Project (product) scheduling and tracking.

(b) Resource and asset allocations.

(c) Macro and micro visibility of all products, either approved or under development.

(d) Special editorial/read-write privileges and rights.

2-3. Electronic document exchange formats. Transfer mechanisms used in e-mail and FTP file transmissions are independent of the actual data file transported. The format of those files, however, is application-specific. To ensure the receiver of files can use the data, a common format must be specified and used by the sender. Guidelines for file formats used in the electronic exchange of documents via e-mail or file transfer are contained in Table 2-1. These file formats are NOT endorsements or mandates for specific vendor products. Many applications besides the original vendor's can read and write these formats. They are intended to represent the most capable, richest functional formats that are widely available and supported. Formats are listed in order of preference.

2-4. Interim methods for electronic staffing. Pending completion of electronic staffing system as described above, the following procedures are to be used—

a. Direct editorial marks in the document. Revision marking is available in Microsoft Word version 6.0.

b. The beta test version of a Web-based DA Form 2028, Recommended Changes to Publications and Blank Forms. This process uses "frames" technology and requires a frames-capable browser. Frames technology can be seen on the Netscape Homepage at http://www.netscape.com. See the help page or Kudos-A-Frames Tutorial. A frames enabled browser is necessary for viewing the beta test at http://155.217.35.75/atimp/e2028beta/e2028beta.htm.

Table 2-1 Electronic Document Exchange Formats

Document Type	Standard/Format	File Name Extension (MIME* type)	Reference Standard
Plain Text	ASCII Text MS Word 6.0 or later	.txt .doc	ISO/IEC 8859-1 Vendor
Compound Document	MS Word 6.0 or later WordPerfect 5.2 or later Acrobat 2.0 or later HTML 3.0 SGML Asymetrix Multimedia ToolBook-CBT Edition	.doc .wpo .pdf .htm .sgm .tbk	Vendor Vendor Vendor IETF FIPS 152 Vendor
Briefing - Graphic Presentation	MS Powerpoint 4.0 or later HTML 3.0	.ppt .htm	Vendor IETF
Image - graphics or photo	JPEG or gif TIFF CGM (graphics only) EPS XBM FAX Group 3 4	.jpg .gif .tif .cgm .eps .xbm .fax	JPEG ISO 10918 gif - Vendor CCITT (ITU-T) FIPS 128 Vendor IETF CCITT (ITU-T)
Motion Pictures/Video	MPEG-1 MPEG-2 MS Video for Windows Quicktime	.mpg .avi .qt or.mov	ISO 11172-2 ISO 13818-2 Vendor
Audio	Audio interchange Windows Waveform Musical Instrument Digital Interface (MIDI)	.aif .wav .mid	ISO 13818-3 ISO 13818-3 MIDI 1.0

* Multipurpose Internet Mail Extension

NOTE: Compound documents contain embedded graphics, tables and formatted text. Not all special fonts, formatting, or features supported in the native file format may convert accurately.

Chapter 3
CD-ROM Publishing

3-1. General. Electronic publishing generally describes the pre-press application of technology to output to a paper media. The intent of this chapter is to offer an application that outputs to a digital media. Recognizing that there are several digital media such as floppy disk, magnetic tape, and videodisks, this chapter is limited to CD-ROM production.

3-2. CD-ROM standards. Adopted standards for TRADOC CD-ROM information products are ISO 10149, 9660, 13346, and 13490. Minimum requirement is ISO 10149 (physical standard) and ISO 9660 (volume and file structure). Refer to Military Handbook 9660 for detail.

3-3. Disc labeling. Use the following disc labeling instructions for both classified and unclassified DOD-produced CD-ROM discs destined for distribution as a final product. Unless specified as "optional" all items should be present on any DOD-produced CD-ROM disc. All information on the label should also be unclassified.

a. Data classification:

(1) Security classification: For discs containing classified information, use the highest classification of any information contained on the disc. Position the classification marking at the top of the disc label, in 18 point bold type with a Sans Serif typeface. All other markings on the label should have a smaller point size than the classification marking. The following standard forms are available as disc labels:

(a) SF 706, TOP SECRET Label for ADP Media.

(b) SF 707, SECRET Label for ADP Media.

(c) SF 708, CONFIDENTIAL Label for ADP Media.

(d) SF 709, Classified Label for ADP Media.

(e) SF 710, Unclassified Label for ADP Media.

(f) SF 711, Data Descriptor Label for ADP Media.

(2) Other protective markings: For discs containing protected information, such as For Official Use Only (FOUO),use at least 12 point bold type with a Sans Serif typeface.

b. Handling caveats: Discs containing any information with handling caveats should comply with the following guidelines:

(1) For discs containing information covered by Public Law 93-579 "The Privacy Act of 1974," the handling caveat phrase "Privacy Act Data, Sec 552a, Title 5, U.S.C." is placed directly below the data classification marking.

(2) Prominently display access or use constraints, such as "copyright," "proprietary," or "limited distribution" on the label.

c. Classification color rings: For discs containing classified information, place a 1/4 inch wide color ring along the outside perimeter of the disc label. The following list provides the ring color for the corresponding classifications:

(1) Yellow . (SENSITIVE COMPARTMENTED INFORMATION)

(2) Orange . (TOP SECRET)

(3) Red .... (SECRET)

(4) Blue ... (CONFIDENTIAL)

d. Producing organization's name: All discs.

e. Classification authority: For classified discs.

f. Declassification date: If applicable.

g. Producer seal/logo: Optional.

h. ISO 9660/compact disc data storage logos: Optional; however, placing the ISO 9660 logo on a disc indicates to the user that the disc is ISO 9660 compliant. It also quickly identifies the disc as a CD-Audio, CD-ROM, CD-I, etc., without having to insert it into a drive.

i. Title of production or disc set, including any disc set numbering schemes, such as 1 of 3: All discs. NOTE: Include markings on classified discs to show that the title is unclassified information (U).

j. Date produced: All discs.

k. Platforms supported: If applicable (example: Windows Version 3.11 or later).

l. Supplemental data formats used: When using any extended or supplemental data formats (examples: XA, MPC, MPC2).

m. Edition: Optional.

n. Volume identification: All discs. This should be identical to the 11 characters of the Volume Identifier (first 11 characters of the ISO 9660 Volume Identifier (32 characters available)) written in the header of the disc. To accommodate the requirements for unique volume identification for discs in CD-ROM jukeboxes, towers, and network systems, use the producing organization's Unit Identification Code (UIC) as the first six characters; the producing organization should then manage/ensure disc uniqueness using the next five characters of the Volume Identifier.

o. Identification number for disc (serial/copy #): For accounting of TOP SECRET or code word discs, optional for other discs.

(1) For TOP SECRET or code word disc accountability, each producer should assign a unique serial number to each title or production release. Additionally, each disc should contain a copy number unique to the serial number.

(2) For accountability of other discs: As needed. Identification Numbers can be used to provide accountability for every disc produced.

3-4. CD-recordables. Items in paragraph 3-3 above also apply to CD-recordable discs. If used, adhesive labels should be frangible (tears if you try to remove it). CD-recordable adhesive labels need to be thin enough to not interfere with the CD-ROM drive and be able to withstand humidity and heat in typical user environments. CD-recordable label printers need to have permanent, smear-proof inks.

3-5. Internal CONTENT.TXT file. For every DOD-produced CD-ROM disc, include a flat ASCII file titled "CONTENT.TXT" in root directory. See Appendix B for formatting information.

3-6. Compact disc guidelines.

a. Software guidelines.

(1) Licensing issues. A major concern in the production and dissemination of CD-ROM discs is software licensing restrictions and costs for the selected authoring/retrieval package. A search and retrieval engine can be used to support those CD-ROMs containing extensive text. This is required to facilitate rapid searches through volumes of information. Authoring software is normally packaged/priced separately from retrieval software, but is specifically designated for a single retrieval engine. Each operating platform supported by the disc may require separate viewers, authoring software, or both. Most authoring/retrieval engines can be purchased in a variety of ways. The following list defines many of the more popular licensing schemes. Any combination of the schemes can be negotiated. Before any purchase, investigate the number of titles, copies, updates, and users affected by the license(s).

(a) Site license: A one-time cost includes all future titles, replicated copies and users. A separate fee or royalty is not required for each user receiving a CD-ROM disc. Example: A site license for authoring and retrieval software may cost $50,000, with no additional charges. This method is usually the most cost-effective if a single package can address all of your CD-ROM publishing needs.

(b) Per title license: A one-time cost and a fixed royalty for each new title produced. A producer pays a fixed fee, and an additional fee each time a new title is produced. Example: Purchasing price is $20,000, each new title costs $10,000.

(c) Per product license: A one-time cost per CD-ROM product regardless of the number of discs replicated or the number of releases. This type of license is usually associated with a unique customer base/type (distribution list) but can grow/shrink as required.

(d) Free runtime licensing: A one-time cost is paid for the authoring software and there are no costs associated with distributing the retrieval engine.

(e) Per user or replicate licensing: A one-time cost is paid for the authoring software and a fee for each user or each disc replicated/distributed must be paid. Example: A producer pays $20,000 for authoring software, then $10 for each user or each disc disseminated. This is the favored approach of vendors but can often be the most costly for producers.

(2) Authoring/retrieval software selection. One of the most important decisions to be made when developing a CD-ROM product is the authoring package/retrieval engine used. There are a large number of government and commercially developed packages available. Any product having a significant amount of text should have a full text retrieval package. There are several packages available that enable producers to easily convert existing paper products to CD-ROM, but they also require more time and effort on the part of the end user to obtain/access required information. Although the catalyst for producing CD-ROM products is often cost effective for the producer; end user acceptance/utilization must be given the highest priority when selecting a package. If the end user does not accept, or cannot effectively utilize the CD-ROM product, then either the paper product must continue to be produced or the end user no longer has access to the information. CD-ROM developers/producers should get their prospective end users involved early in the development cycle. If users feel they have contributed to the development of the product and in the selection of the retrieval engine, they are more likely to accept the product and continue to work with the producers to perfect the product. Approaches/methods for developing standards governing the selection and use of retrieval engines include:

(a) Selecting a single engine or a small set of engines for use.

(b) Compiling a list of minimum capabilities required of any authoring/retrieval system used.

(c) Adopting a data exchange standard. This approach uses a client-server architecture with a standard messaging format so any compliant user interface can query and obtain data from any other compliant server database (example: a command could use its own retrieval engine on any CD-ROM disc complying with the standard);

(d) Standardizing on the actual stored data format with like data being represented consistently (examples: WordPerfect format, SGML, PDF, RTF);

(e) De facto standardizing by limiting the number of organizations allowed to produce CD-ROM titles;

(3) Installation requirements. If data or programs are to be installed on a system, the CD should include an interactive installation routine that allows the user the option of selecting any drive as the destination drive for downloaded files and any drive as the CD drive. If the installation routine software runs under a Windows environment, it should include a de-installation routine that returns Windows, the system's initiation files, and the drives to the pre-installation state. To facilitate manual removal of the CD software, the CD includes a text file that lists the directories created, files copied to drives, and changes made to all Windows and operating system initiation files.

b. Production guidelines (recommendations).

(1) Decision to produce CD-ROM. The production of a CD-ROM can be a lengthy process. Proper planning is a must for proper production and the right decisions made during the planning stage can make or break the success of the project. The following points must be considered before initiating a CD-ROM project:

(a) Decide whether the project is a money making venture or an internal vehicle for boosting efficiency and reducing costs. Have a realistic idea of direct and associated costs and desired results.

(b) Evaluate what, how, and to whom information is to be disseminated. Benefits to the customer/user must be considered in addition to benefits to the producer. Figure out the perishability of the information to be put on the CD-ROM. Ease of retrieval of CD-ROM versus other media, weight/volume trade-offs, urgency of dissemination, and timeliness all need to be integral variables in determining the best approach. Be flexible.

(c) Determine if data used must be integrated, cleaned up, or reformatted. Consider the time, effort, and cost for any needed digital conversion. Formulate all costs and time involved in this effort.

(d) Determine hardware requirements. Evaluate any hardware constraints bearing on the success of the project. Consideration can be given to producing and using the CD-ROM across hardware/operating platforms (example: Windows Version 3.11 or later). Consider this for the production environment as well as the user environment.

(e) Evaluate user acceptance of this type of information. This is the most important step for ensuring a valuable product is developed. Get users involved early in the development cycle.

(f) Determine what production and user software may be required. Is the software available? If not, is there an efficient approach to get what is needed? Look carefully at user fees and licenses.

(g) Evaluate the need for data encryption, serialization, or copyrights. Follow established procedures. Consult with your legal office before including copyrighted or non-freeware/shareware material copyrighted by non-government organizations on your CDs.

(h) Evaluate and readjust the project production and distribution time frame as often as needed. Make sure all steps in the production, replication, and distribution process are considered.

(i) Determine the impact of final packaging. The variety and availability of materials, such as use of color, number of discs per package, or method of distribution, all affect costs and efficiency.

(j) Evaluate the need for, and method of, providing training. Determine options and time needed.

(k) Plan for the impact on maintaining and updating data. Determine the process needed to update. Evaluate redistribution approaches.

(l) Evaluate any similar products. Determine any advantages and disadvantages.

(m) Develop an investment strategy based upon a cost and benefit analysis, comparing CD-ROM dissemination of information with the use of paper medium for distribution.

(2) Commercial CD-ROM replication versus local production break-even analysis tool. When many copies of a CD-ROM are to be produced, one decision to be made is whether to produce CD-ROMs locally (in-house) using one-off machines or to contract the job to a CD-ROM replication company. If time is critical, local one-off production may be the only satisfactory alternative (although one-day turnaround can be obtained from a production vendor). If there is time to have a company replicate the CD-ROM, however, the prime consideration becomes cost. At Appendix C is a tool to assist in identifying the crossover point (number of CD-ROMs) at which it becomes less expensive to use a CD-ROM replication company. If a CD-ROM production-run is below the crossover point, it costs less to produce them locally; if higher than the crossover point, it costs less to have them produced by a CD-ROM replication company.

(3) Legal requirements. All CD production and distribution adhere to the same copyright and legal requirements that the information must meet when distributed in other forms. These requirements are specified in detail in AR 25-30 (The Army Integrated Publishing and Printing Program), and AR 25-1, Chapter 7 (The Army Information Resources Management Program).

(4) Requirements for authenticated departmental publications on CD. AR 25-30 recognizes CD as an official distribution medium. All authenticated departmental publications must follow AR 25-30. See Appendix D for specific handling of authenticated departmental publications on CD. All authenticated departmental publications on CD, including changes, include the authentication block of the appropriate authenticating official. This requirement also applies to authenticated departmental publications that contain other information products (e.g., video). If imaging software that allows the digital scanning of the authentication block is not used as part of the CD, the authentication may appear as text only. In these instances, the authentication includes the assigned authentication block number (for equipment and technical publications and for training and doctrinal publications). Proponents are responsible for assuring that information placed on CDs that requires signature authentication has come from those authorized to sign documents.

(a) Replication requirements. The Joint Congressional Committee on Printing and the Government Printing Office (GPO) considers replication of publications and forms on CD as a printing process. Therefore, all replication containing authenticated departmental publications should be replicated through the Defense Automated Printing Service (DAPS).

(b) Pre-mastering of information for CD may be acquired by the local command or agency separately from disc replication. The proponent acquires mastering and replication of the disc. For authenticated departmental (administrative) publications, U.S. Army Publications and Printing Command (USAPPC) performs the contractual functions for procurement of the CD through DAPS.

(5) Army CD index requirements. Proponents who produce more than three CD products for Armywide distribution maintain and distribute an annual index of CD products for which they are responsible. The index contains sufficient information for end users to request additional copies and to maintain accountability of classified information (if any) contained in the CD. The index is distributed to end users and to the proponent organization's Deputy Chief of Staff for Information Management (DCSIM) or Director for Information Management (DOIM). As an alternative to paper distribution, proponents may place a section on the Office of the Director of Information Systems for Command, Control, Communications and Computers (ODISC4) Homepage; who provides a homepage central file location. Doing so requires compliance with the Government Information Locator System (GILS). Existing indexing mechanisms, the Defense Automated Visual Information System (DAVIS), and the Defense Instructional Technology Information System (DITIS), for visual information products and interactive courseware satisfy this requirement. (For CDs that contain only authenticated departmental publications, a listing of the CD in DA Pamphlet 25-30 satisfies this requirement and already is GILS compliant). At a minimum the index provides:

(a) Title of the CD or set.

(b) CD number.

(c) Title(s) of products contained in the CD.

(d) Classification and protective markings, if higher than unclassified, or the highest classification if both classified and unclassified information are included on the CD.

(e) Proponent name and address and name, address and phone number of a point of contact.

(f) Date of production.

(6) Disc packaging and mailing. There are several options available for packaging a CD-ROM disc for distribution. A choice must be made on both the actual disc container and packaging/mailing container.

(a) Some of the most popular disc containers include: jewel cases, tyvex sleeves, paper sleeves, disc caddies, and multi-disc trays. Paper/tyvex sleeves are the lowest cost containers and are often provided free with the purchase of replicated discs. Jewel cases are fragile, but provide a good mechanism for marking the packaged disc with needed information (such as title, classification, date).

(b) Some of the most popular packaging/mailing containers include: cardboard disc mailers, padded disc mailers, padded envelopes, bubble wrap within an envelope, and envelopes by themselves. Cardboard disc mailers and padded disc mailers usually come with a self adhesive securing strip saving some packaging time and effort but they only provide slightly better protection then regular envelopes. Bubble wrap and padded envelopes provide good protection for discs, especially when jewel cases are used.

(7) CD containers, paper enclosures, and liners. CD containers, such as jewel cases or cardboard cases, can provide information on the front and back cover as well as the two side ribs.

(a) For classified discs, place a 1/4 inch border of the appropriate color on both the front and back covers as well as a 1/4 inch color square on the top and bottom on each of the ribs. Stamp/mark the backside of any sleeve containing a classified disc with the classification of that disc.

(b) Note that marking the CD containers, paper enclosures, or liners does not take the place of 4.3 labeling instructions. If any of the classification markings on the disc itself is covered by the container, enclosure, or liner, then all of the items in 4.3 (except those listed as optional) need to be repeated on the container/enclosure/liner.

c. End-user guidelines.

(1) Minimum end-user system to be supported.

(a) Minimum system requirements are to be used by TRADOC CD-ROM producers as a baseline equipment suite to design their products. See Table 3-1 for HQ TRADOC preferred and supported desktop hardware. Producers should assume TRADOC personnel have access to the minimum Windows environment (80386 processor, A MB RAM, 250 MB hard disk—must have 20 MB free space, EGA color monitor). If producers know their users/customers have a higher level system, then they can design to the higher level. NOTE: The preferred software for electronic staffing and publishing is MS office. See Table 3-2.

(b) Minimum CD-ROM drive specifications. All Environments: 1X CD-ROM drive, ISO 9660 compatible, with appropriate driver software and interface card/ cabling for the computer system being used. A High Sierra compatible drive is not necessarily ISO 9660 compatible although ISO 9660 can read High Sierra format. Also, some MS-DOS PCs only support Level 1 of ISO 9660, which limits the number and type of characters that can be used for file names and directory names. Typical average access times for these drives range from 350 milliseconds (msec) to one second and throughput/ data transfer rate is approximately 150 KBps (Kilobytes per second).

Table 3-1
HQ TRADOC Preferred and Supported Desktop Hardware List

DOD Minimum Configuration	HQ TRADOC Preferred and Supported Hardware Configuration
> or = 66 MHz clock speed	At least 100 MHz Pentium
16M RAM expandable to 32M	At least 32 MB RAM expandable to 64 MB
At least 1 GB hard drive	At least 1 GB hard drive
LAN interface	Ethernet LAN interface
2-PCMCIA type II slots	2-PCMCIA type II, or better, slots
Video controller - minimum 256 colors, 1024x768 pixels	Video controller - minimum 256 colors, 1024x768 pixels, 1MB memory, upgradable; drivers for operating system
CD-ROM Reader	At least 6X CD-ROM Reader
3.5" floppy drive	3.5" Floppy Drive capable of reading and writing both 1.44MB and 720KB diskettes
2-parallel and 2-serial ports	2-parallel and 2-serial ports
Pointing device with a minimum of two buttons	Pointing device
17" color monitor	15" Color Monitor, SVGA
	16-bit sound card (for multimedia applications) and drivers for operating system
	3 PCI expansion slots

Table 3-2
HQ TRADOC Preferred and Supported Desktop Software and Operating System List

Category	HQ TRADOC Preferred and Supported Desktop Software and Operating System
1. Desktop Client Operating System	Microsoft NT
2. IP Protocol Stack (Includes TELNET)	Microsoft
3. Office Suite	FULL SUITE: Microsoft Office Pro WORD PROCESSING: Word SPREADSHEET: Excel PRESENTATIONS: PowerPoint DATABASE: Access PROJECT MANAGEMENT: Project
4. Office Management	* Microsoft Exchange ** Schedule+
5. Internet Browser (Includes FTP and Newsgroups)	*** MS Explorer
6. Forms	FormFlow
7. Multimedia Authoring	Asymetrix Multimedia ToolBook-CBT Edition

* Must be DMS compliant and/or upgradable at no cost to DMS compliance.
** Provided with MS Exchange and DMS-compliant version.
*** Provided as a component of NT Workstation 4.0.

Chapter 4
Doctrine and Training Development Automation Tools

4-1. General. An effective organization needs immediate access to both its current operating information and its historical records. TRADOC elements are implementing a digital means to accomplish this mission for the doctrine and training products, information, and records they provide the Army. This section of the pamphlet describes the general aspects of the effort.

a. Migration from paper-based to electronic information. Doctrine and training information and products within the Department of Army are developed and disseminated using evolving technology and applications/systems. These systems are currently being developed and support the Army's transition from paper-based to digital-based doctrine and training development and distribution.

b. Technology. The technology and systems discussed in this section are utilized by Army Doctrine and Training developers in the execution of their creation and production of doctrine and training information and products. As these systems meet functional requirements and hardware and networks are installed and become operational, their use is mandatory by all users including contractors. The continued enhancements to these systems and adaptation of technology improves interoperability, facilitate information exchange, provide a means for information sharing, redundancy control, minimize information handling and improve information integrity.

c. Sharing information. The development and implementation of standardized, automated information systems provides for the sharing of proponent produced and approved doctrine and training information and products. These systems are to be mutually dependent. Information developed in one system is to be shared with and used by other systems. This improves the Army's capability to develop information once, and use it repeatedly, saving time and improving standardization. Connectivity between these systems is based on protocols and data standardization procedures mandated by the Army Technical Architecture (ATA). Adherence to this common architecture ensures data is stored in a manner that facilitates the widest possible uses and maintain the synchronization necessary in the future.

d. Information integrity. Doctrine and training/task proponents are responsible for the management of content, accuracy, completeness, relevancy, and subsequent manipulation of their information as they continue to use emerging systems and technologies to support the Army's movement to digitization of information.

e. Installation guidance. Using organizations must take the initiative to obtain and install the necessary hardware and networks, get the appropriate systems installed in their organization, and train the system users. Systems operations training is obtained through the Army Training Support Center (ATSC).

4-2. Guidance.

a. Training products guidance. Policy, procedures, and formats for management and development of training products and materials is established and described in TRADOC Reg 350-70, Training Development Management, Processes, and Products, and TRADOC 350-70-series supporting pamphlets. This regulation also provides a glossary of training and training development terms for communication.

b. Doctrine products guidance. Policy and procedures for developing doctrine products is established in TRADOC Reg 25-30, Preparation, Production, and Processing of Armywide Doctrine and Training Literature, and TRADOC Reg 25-32, TRADOC Doctrinal Literature Master Plan.

4-3. Technology and systems. This section provides information on the tools, when completely developed fully implements electronic dissemination of doctrine and training information within the Army. This paragraph provides general information on these initiatives to assist in determining which systems should be installed in your organization. These systems are fully compatible to totally implement electronic dissemination of doctrine and training related information within the Army. It is the doctrine and training/task proponents responsibility to keep current on the capabilities of the latest version of each of these systems. To accomplish this, the training/task proponents should assign a POC for each system and give them the responsibility for coordinating with the system program managers at ATSC or Center for Army Lessons Learned (CALL) as appropriate.

a. Automated Systems Approach to Training (ASAT). The ASAT provides a relational doctrine and training development and management system with seamless links to other Army Training XXI initiatives. The ASAT:

(1) Automates six major functional areas: Doctrine development, determining TD requirements, managing TD, producing collective training products, and producing individual training products, per TRADOC Reg 25-30 and training development management as delineated in TRADOC Reg 350-70.

(2) Is used by doctrine and training developers, TD managers, and contractors wherever these functions are performed.

(3) Currently can be used to produce program directives, field manuals, mission training plans, and drill books and has an unlimited reporting capability of information contained in the system.

(4) Capabilities will be expanded to include development of other training products such as Combined Arms Training Strategies (CATS) and Warfighter training support packages.

(5) Provides project execution and milestone capability, electronic staffing, media linkages at the paragraph or task and task performance step/measure level. Doctrine and training information on the system are totally integrated including crosswalk between the individual and collective task-based information.

(6) Is integrated with the Standard Army Training Systems (SATS), the Automated Instructional System-Redesign (AIMS-R) and the Army Training Digital Library (ATDL) and serves as the task-based foundation for follow-on training development and training.

b. Automated Instructional Management System Redesign (AIMS-R). AIMS-R provide the capability to develop, administer and monitor resident and nonresident individual training during peacetime and mobilization. AIMS-R:

(1) Users are training developers, resource management, training management, trainers, and training support personnel.

(2) Automates processes necessary for course design/development (vice ASAT), student management, gradebook management, testing and evaluation of students (vice ASAT), inventory management, worldwide distribution and printing of instructional and testing materials, scheduling of classes, training events, and resources, to include impact analysis of "what if," and archival of historical records; and career education and training status tracking.

(3) Automates course design/development and testing and evaluation of students IAW TRADOC Reg 350-70.

(4) Is scheduled to replace the following information systems sometime in the future:

(a) The current resident training management system, Automated Instructional Management System (AIMS).

(b) The current nonresident training management system, TRADOC Educational Data System - Redesign (TREDS-R).

(c) Program of Instruction Management Module (POIMM).

(d) TRADOC Automated Training Scheduling System (TATSS).

(5) Provides individual training development information and products to units via SATS.

c. Program of Instruction Management Module (POIMM). The POIMM is a development tool that provides the training/task proponents with a means for compiling a digitized Program of Instruction (POI) and Training Requirements Analysis System (TRAS) documentation.

d. Standard Army Training System (SATS). SATS application automates the unit training management and execution outlined in FM 25-100 and FM 25-101. SATS:

(1) Users are unit trainers from platoon through corps.

(2) Provides current doctrine and training information/products to unit trainers.

(3) Users are able to take the information off line and manipulate it for other uses but the application allows modification of the provided doctrine or training/task proponent information.

e. Training Module Executive Management Information System (TEXMIS). TEXMIS is the Army's primary source for doctrine and training information and products. It offers the capability to automatically transfer data between Army proponent schools, units, and other DA automated systems. The TEXMIS central repository contains relational information from the Standards in Training Commission (STRAC), the Army Cost Factor Handbook, the Combined Arms Training Strategy (CATS), Modified Tables of Organization and Equipment (MTOE), ASAT-derived task and doctrine information, and AIMS-R developed training materials and products. TEXMIS will be operational by the end of 1st Qtr, FY97.

(1) Training/task proponents use ASAT to transmit to and from TEXMIS. Connectivity is accomplished either through the Internet and/or modem-to-modem connections. It is the responsibility of doctrine and training/task proponents to keep their information/products stored in TEXMIS current.

(2) Units use SATS to transmit to and from TEXMIS. Connectivity is accomplished either through the Internet and/or modem-to-modem connections. It is the responsibility of the unit to keep their information/products stored in TEXMIS current.

(3) Training/task proponents and schools use AIMS-R to transmit to and from TEXMIS. Connectivity is accomplished either through the Internet and/or modem-to-modem connections. It is the responsibility of the training/task proponent to keep their information/products stored in TEXMIS current.

(4) TEXMIS information is also accessible via the Army Training Digital Library (ATDL). While TEXMIS is the repository for doctrine and training information, the ATDL provides the pointer to TEXMIS (transparent to the users). Both TEXMIS and the ATDL are managed by ATSC to ensure both the fidelity and accessibility of the data.

(5) To obtain access proponent/users must contact the TEXMIS program manager at ATSC. Basic users with a bona fide need will be given read access. Individuals without a need to access the database or who are not registered will not be able to gain entry. The majority of the Army will never directly concern themselves with the functions or contents of TEXMIS other than as directed by the interface built into the application they are using at the moment.

(6) There are many other databases, systems, and/or applications that currently take advantage of doctrine and training information. Users currently accomplish this by copying the information from the ATSC produced CD-ROM. TEXMIS replaces the need for the CD-ROM by providing the most current collective and individual task information on-line.

f. Army Training Digital Library (ATDL). The Army Training Digital Library (ATDL) is the Army's electronic library for doctrine and training information and

products. It serves the Army as a library without walls taking advantage of the speed and flexibility afforded by the Internet. It provides world-wide users access to the latest, approved doctrine and training products with an immediacy previously unknown. It is the single certified World Wide Web (WWW) site for Army Field Manuals (FM). Users obtain information by accessing it through the WWW at URL: http://www.atsc-army.org/atdls.html.

g. Lessons learned information tool. The Center for Army Lessons Learned Collection and Observation Management System (CALLCOMS) is a confederation of databases and systems operating through a common gateway that serves as a source for lessons learned information. Users desiring this information must currently access the CALLCOMS. Eventually this information will be available through the ATDL.

4-4. Digitization of existing doctrine and training products. ATSC has a capability of converting legacy doctrine and training products/information into digital form for inclusion in above information systems. This process involves digital scanning of legacy, paper-based products previously certified and approved by the doctrine or training/task proponent. Doctrine and training/task proponents should contact ATSC for assistance in this digitization effort.

Chapter 5
Archiving

5-1. General. This chapter specifies detailed functions that Records Management Applications (RMAs) must perform. The requirements are presented in plain language to allow maximum flexibility in software development while ensuring responses can be tested. They are intended to provide a constraint and to bind the requirement to ensure standardization, but are not intended to specify data type format. Standards for managing information as records are taken from DOD STD 501 5.2, Design Criteria Standard for Records Management Application Functional Baseline Requirement. Any automated system developed within TRADOC that creates records must meet these requirements.

5-2. Identifying records. Identifiers must be assigned based on Modern Army Recordkeeping System (MARKS), and must be keyed to a file category (number) with an assigned retention period. RMAs must:

a. Assign a unique computer-generated record identifier to each record, both electronic and non-electronic.

b. Assign a different record identifier to any new versions of a previously filed record.

c. Not permit modification of the record identifier once assigned.

d. Have the capability to associate and link a record to its attachments.

e. Provide the capability to store multiple components of a single record and to retrieve all components of a multi-part record.

f. Provide the capability to record the following profile data (metadata) for all records:

(1) Subject.

(2) Date of record.

(3) Addressee(s).

(4) Media type.

(5) Record format.

(6) Location of record.

(7) Document creation date.

(8) Author or originator.

(9) Originating organization.

g. Provide the capability to edit the above metadata prior to filing the record.

h. Provide the capability to output for viewing, saving, or printing the record profile information (metadata) identified in paragraph 5-2f, above.

i. File records and assign disposition.

j. Provide the capability for only authorized individuals to create, add, and delete organizational record categories and their codes. Each category code must link to its associated category and to its higher level category code(s).

k. Provide the capability to designate vital records categories.

l. Provide only authorized individuals the capability to reverse the designation of a vital record category once the designation has become obsolete.

m. Provide the capability to select and assign a file code to a record.

n. Provide the capability for only authorized individuals to create, add, and delete disposition instructions and their associated codes. Each disposition code must link to its associated disposition instruction.

o. Provide the capability for only authorized individuals to assign a disposition instruction code to a record category.

p. Provide the capability for only authorized individuals to suspend disposition instructions for individual files or record categories.

q. Provide the capability for only authorized individuals to limit the file codes available to a user or work group.

r. Provide the capability to output for viewing, saving, and printing, the organizational record categories and category codes.

s. Provide the capability to output for viewing, saving, and printing, the disposition instructions and disposition codes.

t. Provide the capability for only authorized individuals to modify the metadata (values of the record profile attributes) of stored records that have not been otherwise specified as unchangeable.

5-3. Storing records. RMAs must—

a. Store electronic records.

b. Maintain the integrity of the record as it was received, and not change the format of records they store.

c. Provide a repository for electronic records and prevent unauthorized access to the repository.

5-4. Screening records. RMAs must—

a. Provide for viewing, saving, and printing list(s) of records within record categories based on disposition instruction code and/or record category code to identify records due for disposition processing. The information contained in the list(s) shall be a limited set of record profile attributes.

b. Identify files scheduled for cutoff, and present them only to the authorized individual for approval. RMAs must not allow any additions or other alterations to files that have been cutoff.

5-5. Retrieving records. RMAs must—

a. Maintain the following record profile information (metadata) for all records:

(1) Record identifier.

(2) File code.

(3) Subject.

(4) Date of record.

(5) Addressee(s).

(6) Location of record.

(7) Media type.

(8) Record format.

(9) Document creation date.

(10) Author or originator.

(11) Originating organization.

b. Search for records using any combination of the metadata specified in paragraph 5-5a above, as well as file metadata identified below and in paragraph 5-9b, as retrieval criteria:

(1) Disposition instruction code.

(2) Disposition cutoff date.

(3) Disposition action date.

(4) Disposition action code (transfer or destroy).

(5) Vital record code.

RMAs must allow the user to specify whether or not exact match of case is part of the search criteria, allow for specifying partial matches for multiple word fields such as subject and date, and allow designation of "wild card" fields or characters.

c. Present the user a list of records meeting retrieval criteria, or notify the user if there are no records meeting the retrieval criteria. The information contained in the list must be a limited set of record profile attributes.

d. Provide to the user's workspace, copies of records selected from the list of records meeting the retrieval criteria in the format in which they are stored.

5-6. Copying records. RMAs must—

a. Never allow modification of the content of a stored record.

b. Provide the capability to copy a record or records in a file or category into a user work space for viewing or other use. Filing of the revision of the copy or conversion of format or medium must generate a new record.

5-7. Transferring records.

a. Using the disposition instruction for the record category, the RMA must identify and present, only to an authorized individual, those record categories eligible for transfer.

b. For a record category approved for transfer, RMAs must output the pertinent records and associated profiles. RMAs must delete the records and associated profiles IAW paragraph 5-9c, below.

c. For records approved for transfer, RMAs must provide the capability for only authorized individuals to suspend the selection of records and related profile until successful transfer has been confirmed.

5-8. Destruction of records.

a. Using the disposition instruction for the record category, the RMA must identify and present, only to an authorized individual, those record categories eligible for destruction.

b. RMAs must require a second confirmation prior to the destruction operation.

c. RMAs must delete records approved for destruction in a manner such that the records cannot be physically reconstructed.

5-9. Electronic mail (e-mail). E-mail messages are treated the same as paper records. An e-mail message must be designated a record by the originator if it is related to the organization's mission or business or it is used in other official actions. RMAs must:

a. Store and manage designated e-mail transmissions, including attachments, whether sent or received, as records.

b. Capture and automatically store the following transmission data as part of the record profile when an e-mail is filed as a record:

(1) The e-mail name/address of the sender.

(2) The e-mail name(s)/address(es) of the addressee(s). The e-mail name(s)/address(es) of other recipients.

(3) The date and time the message was sent.

(4) The subject of the message.

(5) For messages received, the date and time the message was received. RMAs must not allow manual editing of these metadata.

c. Store the attachments to an e-mail record and to associate and link the attachment with the e-mail record.

d. Provide the capability to store distribution lists as required to ensure identification of the sender and addressee(s) of messages that are records.

5-10. Access control. RMAs must—

a. Control access to records based on record categories and files, and user account information.

b. Control access to the transfer and destroy functions based upon user account information.

c. Control access to audit functions based on user account information.

5-11. System audits.

a. RMA audit utilities must provide an account of records capture and preservation activities to assure the reliability and authenticity of a record.

b. RMA audit utilities must provide a record of transfer and destruction activities to facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, possible compromise of sensitive information, or denial of service.

c. RMAs must provide the capability to store audit data as a record.

d. The following information must be reported on demand:

(1) Total number of records captured.

(2) Number of records captured by record file code.

(3) Number of accesses by record file code.

e. The following information must be logged for deletions:

(1) Record identifier.

(2) Record category.

(3) User account identifier.

f. RMAs must allow only authorized individuals to enable/disable the audit functions and to backup and remove audit files from the system.

5-12. System management requirements. The following are functions typically provided by the operating system or a Database Management System (DBMS). They are also considered requirements to ensure the integrity and protection of organizational records. They must be implemented as part of the overall records management system even though they may be performed externally to a RMA.

a. Backup of stored records. The system must provide the capability to produce, on demand, periodic backup copies of all records managed by RMAs at intervals specified only by authorized individuals.

b. Storage of backup copies. The method used to backup RMA database files must provide copies of the data that can be stored off-line at a location(s) to safeguard against loss of records, record profiles, and other records management information due to system failure, operator error, disaster, or willful destruction.

c. Recovery/rollback capability. Following any system failure, the backup and recovery procedures provided by the system must provide the capability to complete updates (records, record profiles, and any other information required to access the records) to RMAs, ensure that these updates are reflected in RMA files, and assure that any partial updates to RMA files are these updates are reflected in backed out. Also, any user whose updates are incompletely recovered, shall, upon next use of the application, be notified that a recovery has been executed. RMAs must also provide the option to continue processing using all in-progress data not reflected in RMA files.

d. Rebuild capability. The system must provide the capability to rebuild forward from any backup copy, using the backup copy and all subsequent audit trails. This capability is typically used to recover from storage media contamination or failures.

e. Storage availability and monitoring. The system must provide for the monitoring of available storage space. The storage statistics shall provide a detailed accounting of the amount of storage consumed by RMA processes, data and records. The system must notify only authorized individuals of the need for corrective action in the event of critically low storage space.

5-13. Additional baseline requirements. The following records management requirements that must be implemented by the organization, but not necessarily by the RMAs.

a. Electronic calendars and task lists. These sometimes qualify as organizational records. If the RMA being acquired does not have the capability to extract them from the software application that generates them, intermediate procedures must be implemented to enable those records to be managed by the RMA.

b. External e-mail. Some organizations use separate e-mail systems for internet e-mail or other wide area network e-mail. These records must be handled as any other e-mail records. If the RMA being acquired does not provide the capabilities specified in paragraphs 5-9a to 5-9d, processes or procedures must be implemented to enable these records to be managed by the RMA.

c. Ability to read and process records. Since RMAs are prohibited from altering the format of stored records (para 5-3b), the organization must ensure that it has the ability to view, copy, print, and if appropriate, process any record stored in RMAs for as long as that record must be retained. The organization may meet this requirement by (1) maintaining the hardware and/or software used to create or capture the record, (2) maintaining hardware and/or software capable of viewing the record in its native

format, (3) ensuring backwards compatibility when hardware and/or software is updated, or (4) migrating the record to a new format before the old format becomes obsolete. Any migration must be controlled in order to ensure continued reliability of the record.

d. Classified and other sensitive records. If required, the acquisition activity must specify requirements and/or acquire additional capabilities for the management of security classified records, records that contain Privacy Act information, records exempt from FOIA, or any other records that require special access control or handling. The using organization must implement special procedures to comply with legal and regulatory requirements for those records.

5-14. Center for Army Lessons Learned Collection and Observation Management System (CALLCOMS). The CALLCOMS model, developed at Fort Leavenworth, is an example of a system engineered with the use of existing systems standards. It is described in recognition of TRADOC's role in support of the warfighter. This description is included to help systems developers with the planning process and show the level of technical detail required in the automation process. CALLCOMS is a Windows-based, open system, open database connectivity (ODBC) compliant, multi-user, scaleable database application. The objective application must support operations in a SQL client/ server environment; provide an object oriented intuitive and easily understandable graphics user interface (GUI) for data entry and retrieval; effectively process, analyze and manage collected information; improve communications hierarchy; and, significantly decrease the turnaround time from input to use of data.

a. Standards in the server environment. The Server Environment consists of a Master Database Server and a Web Interfaced Server. A potential also exists to employ a Remote Local Area Network (LAN) server which hosts an organization's network and is possibly linked to the Master Database Server and/or to the Web Interfaced Server. Standards in the aforementioned server environments are:

(1) Remote LAN environment - Minimally consists of a file server.

(2) Master database server environment - Database engine running on a Windows NT server or Sun minicomputer with the Sun Solaris operating system. (NOTE: Tests are being conducted regarding the robustness of each platform for this environment.)

(3) Web interfaced server - Database engine running on Windows NT server.

b. Assumptions in the client environment. The Client Environment is defined as an intelligent workstation within a LAN or a standalone desktop PC/laptop computer.

(NOTE: Assumptions are based on current personal computer systems within TRADOC. As upgrades to these systems progress, it is the intent of this application to be able to fully interact with: (1) a graphic users interface (GUI); (2) enhanced display screens utilizing hi-resolution SVGA monitors displaying 024x768 pixels that can accommodate 16.7M colors; (3) modem connectivity that is user configurable and communicates by the fastest bps available (currently v. 34 as a minimum); and (4) SLIP/PPP access to the master database using industry standard TCP/IP connections).

c. Export of data to external databases. CALLCOMS must support information exchange with the current and follow-on versions of the Joint Universal Lessons Learned System (JULLS). This function must support the capability to export filtered information. The intent of this function is to provide the user with a intuitive interface that must allow the creation of a data file containing user determined delimited information. Additional supported export formats are: comma delimited ASCII and a word processing format to be determined (either Word or Word Perfect).

d. Import of external source data into database. CALLCOMS must support information exchange from the current and follow-on versions of the JULLS, as well as receive information from common delimited ASCII files. This function must support the capability to import and selectively place information into a predetermined table's field locations. Application intelligence must identify and populate all required fields with the default value of "unknown" when blank. Additionally, all fields that perform an internal calculation for the generation of record identification or the like must perform this function as part of the import process. The intent of this function is to provide the user with a intuitive interface that must allow the receipt of data from JULLS and other data formats. The goal is to provide a flexible information exchange dialog backed by application and intelligence. Additional required import formats are: comma/tab/character delimited ASCII, Fixed ASCII, DBF, XLS, WK1.

5-15. Document conversion.

a. Document conversion is typically viewed as converting paper documentary material to a digital form, although conversion from paper to microform, digital to microform, digital to digital, and other types of conversion are also common. Because of the rapidly changing and emerging conversion technologies, there is a need to exercise greater discipline in acquisition of automated document conversion equipment, systems, and services. All levels of DOD management with acquisition responsibility should consider the following questions related to document conversion business decisions:

(1) What documents, if any, must and must be converted? For what mission or business reason(s)?

(2) Who decides?

(3) How must those selected documents be converted?

(4) When can selected documents be converted? What criteria are needed to guide scheduling, staging, and phasing of document conversion?

(5) What workflow issues must be resolved during lengthy document conversion efforts?

(6) What are the short-term and long-term (measured by the lifetime of a document) costs of conversion? What benefits are qualified and quantified?

b. Records management defines the policy and provides the structure for managing the life-cycle of information contained in records, regardless of medium of storage (i.e., paper, film, magnetic media). Electronic document management defines a subset of information handling concerned with capturing, retrieving, converting, storing, and disseminating digital forms of information. Automated document conversion (ADC) management focuses on the conversion of documents (analog or digital) to the desired digital formats.

c. The Department of Defense has published an Automated Document Conversion Master Plan which focuses on conversion from paper/microform (analog) to digital formats, although the principles and guidelines apply equally to digital-to-digital and other types of document conversion. It describes a document conversion strategy that is responsive to mission and business requirements. It also confirms the technical standards to which conversion output products (converted documents) must comply. Technical standards specifying document output formats must evolve. Conformance to the technical standards increases the utility of converted documents to the organization.

d. The Department of Defense is committed to the establishment of a standards-based framework for defining technical architectures that will help ensure interoperability, portability, and scalability of its information systems. The standards identified as most suitable for DOD ADC systems will move the Department toward open/non-proprietary systems. All ADC systems must use these standards or provide a business case analysis for using proprietary standards as well as a migration strategy to open systems. The Automated Document Conversion (ADC) Master Plan approved and submitted to Congress on April 3, 1995 presents document conversion as an activity within the records management business process and will be published as a DOD records management publication. The proposed publication, DOD 5015.2-P, ADC Master Plan, may be reviewed at URL http://www.dtic.dla.mil/c3i/recmgmt.html.

e. The document conversion role of DOD Component Commanders, Managers, Records Officers, and Document Custodians is to:

(1) Implement DOD policy to maintain, protect, and preserve organization records.

(2) Determine the component-unique mission and business needs for document conversion.

(3) Support efforts to improve the accessibility of documents.

(4) Validate the component-unique mission and business need, and justification for document conversion.

(5) Convert documents internally, use centralized DOD conversion services, or contract out for conversion services, ensuring employment of the most cost-effective conversion approach consistent with the business justification.

f. These officials—

(1) Coordinate with the functional manager, records officer, systems support officer, and legal officer to determine eligibility of an original document for conversion.

(2) Determine if the original or the converted document must be the organization record, IAW the organization's published records disposition schedules approved by the Archivist of the United States.

(3) Consider the long-term financial costs of managing documents in either their original medium or in their converted medium.

(4) Consider the stability and life-cycle of the proposed medium of storage for converted documents.

(5) Consider the life-cycle of the hardware and software used to store, retrieve, and manage a converted document throughout its life.

(6) Select documents for conversion based on the information value, need to share the information in an electronic environment, and number of times the information must be accessed over its life.

Appendix A
References

Section I
Required Publications

AR 25-1
The Army Information Resources Management Program

AR 25-3
Army Life Cycle Management of Information Systems

AR 25-30
The Army Integrated Publishing and Printing Program

AR 25-400-2
The Modern Army Recordkeeping System (MARKS)

AR 310-25
Dictionary of United States Army Terms

AR 310-50
Authorized Abbreviations, Brevity Codes, and Acronyms

AR 340-9
Office Symbols

AR 380-19
Information Systems Security

DA Pam 25-30
Consolidated Index of Army Publications and Blank Forms

TRADOC Reg 25-30
Preparation, Production, and Processing of Armywide Doctrinal and Training Literature (ADTL)

TRADOC Reg 350-70
Training Development Management, Processes, and Products

Section II
Related Publications

Automated Document Conversion Master Plan, Version 1.0, April 1995, published by the Office of the Assistance Secretary of Defense (Command, Control, Communications, and Intelligence/Information Management)

Federal Information Processing Publication (FIPS PUB) 1-2, Code for Information Interchange, its Representations, Subsets, and Extensions (American Standard Code for Information Interchange (ASCII)

International Organizations for Standardization (ISO) 9660: 19990, Volume and File Structure of CD ROM for Information Interchange

ISO Draft International Standard (DIS) 13490, Volume and File Structure of Read Only and Write Once Compact Disc Media for Information Interchange

MIL-PRF-2800A(JCALS), Digital Representation for Communication of Product Data: Initial Graphics Exchange Specification (IEGES) Application Subsets and IGES Application Protocols

MIL-PRF-28001B(JCALS), Markup Requirement and Generic Style Specifications for Electronic Printed Output and Exchange of Text (Standard Generalized Markup Language (SGML))

MIL-PRF-28002B(JCALS), Requirements for Raster Graphics Representation in Binary Formal (Group 4 Raster Scanned Images)

MIL-PRF-28003A(JCALS), Digital Representation for Communication of Illustration Data: Computer Graphics Metafile (CGM) Application Profile

ISO 10918, Joint Photographic Experts Group (JPEG) 9600 bits per second V.32

ISO 13818, Motion Picture Experts Group (MPEG), MPEG 2 digital motion compression standard

Mil-Handbook 9660: Department of Defense Handbook, DOD-Produced CD-ROM Products, dated 1 December 1995, by the Defense Information Systems Agency

Multimedia Extensions to the DOD Minimum Desktop Configuration, Edition 2, April 23, 1996, published by Defense Information Systems Agency

Section III
Referenced Forms

DA Form 260	Request for Printing
SF 706	TOP SECRET Label for ADP Media
SF 707	SECRET Label for ADP Media
SF 708	CONFIDENTIAL Label for ADP Media
SF 709	Classified Label for ADP Media
SF 710	Unclassified Label for ADP Media
SF 711	Data Descriptor Label for ADP Media

Appendix B
CONTENT.TXT File

B-1. Format. Use 80 or less characters per line, with a hard return (ASCII Carriage Return - Line Feed combination (CRLF)) at the end of each line. Introduce each new information block using descriptors (such as "DISC TITLE:") typed in all capital letters, beginning in column one of their line. Use upper and lower case for associated data.

B-2. Structure. For consistency, use all the following descriptors, although the associated information is optional:

TITLE: State verbatim the name by which the disc is known, including any disc set numbering schemes, such as 1 of 3. Do not include any superfluous descriptions or qualifiers.

EDITION: The version of the title.

VOLUME IDENTIFIER: All discs. This should be identical to the 11 characters of the Volume identifier (first 11 characters of the ISO 9660 Volume Identifier (32 characters available)) written in the header of the disc. To accommodate the requirements for unique volume identification for discs in CD-ROM jukeboxes, towers, and network systems, use the producing organization's Unit Identification Code (UIC) as the first six characters; the producing organization should then manage/ensure disc uniqueness using the next five characters of the Volume Identifier.

ORIGINATOR: The name of an organization(s) or individual(s) that developed the data (see definition of contributed by). If the names of editors or compilers are provided, follow each name by "(ed.)" or "(comp.)," respectively.

CD PUBLICATION DATE: The date when the disc was published or otherwise made available for release.

SECURITY CLASSIFICATION: Name of the security restrictions on the disc. Use the highest classification of any information on the disc.

CLASSIFICATION AUTHORITY/SECURITY CLASSIFICATION SYSTEM:
Name of the classification system. State/reference the actual classification authority or "Multiple Sources" if appropriate. Use "N/A" for unclassified discs.

SECURITY HANDLING DESCRIPTION: Additional information about the restrictions on handling the disc.

DECLASSIFICATION DATE: Provide the date the disc becomes declassified. This is either the last declassification date of any material on the disc, or Originating Agency Determination Required (OADR) if appropriate. Use "N/A" for unclassified discs.

TIME PERIOD OF CONTENT: Time period(s) for which the data on the disc is valid. Select one of the following methods:

SINGLE DATE/TIME: Method of encoding a single date and time.

CALENDAR DATE: The year (and optionally month or month and day).

TIME OF DAY: The hour (and optionally minute or minute and second).

MULTIPLE DATES/TIMES: Means of encoding multiple individual dates and times.

DATA DESCRIPTION:

CALENDAR DATE: as above.

TIME OF DAY: as above.

RANGE OF DATES/TIMES: Means of encoding a range of dates and times.

BEGINNING DATE: The first year (and optionally month or month and day) for which the data is valid.

BEGINNING TIME: The first hour (and optionally minute, or minute and second) of the day for which the data is valid.

ENDING DATE: The last year (and optionally month or month and day) for which the data is valid.

ENDING TIME: The last hour (and optionally minute and second) of the day for which the data is valid.

OPERATING ENVIRONMENT: State the minimum operating system and version, and any other hardware/software requirements.

ACCESS CONSTRAINTS: Restrictions and legal prerequisites for accessing the data. These include any access constraints applied to assure the protection of privacy or intellectual property, and any special restrictions or limitations on obtaining the data.

USE CONSTRAINTS: Restrictions and legal prerequisites for using the data after access is granted. These include any use constraints applied to assure the protection of privacy or intellectual property, and any special restrictions or limitations on obtaining the data.

ABSTRACT: A brief narrative summary describing the CD product/data and its purpose.

ORDERING INSTRUCTIONS: State specifically how to request copies of the CD.

FEES: The fees/terms for receiving the disc.

POINT OF CONTACT: Contact information for an individual and organization that is knowledgeable about the data on the disc.

CONTACT PERSON
CONTACT ORGANIZATION
CONTACT ADDRESS
CONTACT VOICE TELEPHONE
CONTACT FACSIMILE TELEPHONE
CONTACT E-MAIL/INTERNET ADDRESS

MAINTENANCE AND UPDATE FREQUENCY: State plans for product enhancements, schedule of updates, termination of product support or any other related information.

ORIGINATOR COMMENTS: Provide any comments desired by the originator of the CD or products on the CD.

DOCUMENT IDENTIFICATION: List the number, title, date, and originator of each document or product found on the disc. (This and the following document abstract section can be repeating pairs).

DOCUMENT ABSTRACT: Provide a brief narrative describing each document or product on the disc. (This field and the document identification field can be repeating pairs for every document/product found on the disc).

END OF CONTENT.TXT FILE.

Appendix C
Break-Even Analysis Tool (Commercial CD-ROM Replication vs Local Production)

C-1. Replication company charges.

a. The price charged by a CD-ROM replication company is divided into two categories: fixed price and variable price. The fixed price is the same regardless of how many CDs are produced. The variable price is equal to the number of CD-ROMs produced times the total "per CD-ROM" price. The CD-ROM replication company may identify just the total fixed price and the total "per CD-ROM" price or it may itemize the prices. If itemized, you need to identify fixed prices and the "per CD-ROM" prices. The fixed price is the total of the fixed price components for a production run. The "per CD-ROM" price is the composite of the "per CD-ROM" price components.

b. Many replication companies have block rates; for example, one rate for up to 2,000 CD-ROM discs and another rate for 2,000-5,000 which permits greater volume discounts. This analysis needs to be accomplished for each block.

C-2. Break-even number. The following equations are used to determine the CD-ROM break-even number. If the planned production run is larger than the break-even number, the production can be contracted to a CD-ROM replication company. If it is less, the CD-ROMs can be produced locally as one-offs.

NOTE: For the purpose of this equation/example, it is assumed that the producer currently has the capability in-house to produce.

Break-even # = FcC/(ADo = Pdc)

Break-even # = ((1 + S) x FcC)/(ADo - ((1 + S) x Pdc))) (when a surcharge is applied)

FcC - Fixed Charges, Commercial: This is the total of one-time fixed costs charged by the CD-ROM replicator company. Fixed costs include the substantial "start up" costs associated with developing a CD-ROM template (glass master and metal press). It may also include a single charge for etching sequential numbers (serialization) on every disc.

Pdc - Per Disc Charge, Commercial: This is the CD-ROM replication company charge for each CD-ROM produced. It may be provided as a total or may be calculated by adding the following together:

— Charge per disc

— Charge for serialization per disc (may be fixed)

— Charge for printing each included booklet

— Charge per package/container (may be included in disc charge)

— Charge to produce/install liner (may be included in disc charge)

— Charge for mailing each CD-ROM back to the publisher

S - Surcharge: This is the total of surcharges (a percentage of the total commercial charges) levied by contract middlemen; for instance, the Government Printing Office or the Defense Automated Printing Service. Some contracting vehicles should not require a surcharge.

ADo - Average Disc Cost, one-offs. This is the only cost relevant to producing CD-ROMs locally. It is the cost incurred by you, the producer, for each one-off produced. It is the sum of the following:

— Cost per CD-ROM one-off blank (the primary cost consideration)

— Cost per package/container

— Cost per label materials

— Cost per liner materials

— Cost per booklet materials

— Average manpower cost per disc to write to the one-off, make the labels, liner, and booklet and assemble each package.

C-3. Example.

Fixed Charges, Commercial = $2,500.00

Per Disc Charges, Commercial = $3.00

Surcharge = 10%

Average Disc Cost, One-off = $16.00

Break-even # = ((1 + .1) x $2,500)/($16 -((1 + .10) x $3) = 216.6

Therefore, if you need 217 or more copies, you should contract out to a replication company. If you need less than 217 copies, you should produce the discs in-house.

Appendix D
Authenticated Departmental Publications on Compact Disc

Requests for CD products greater than 2x speed (the most common Army speed for text-based products) should be accompanied by clear identification of the audience and certification on DA Form 260 that the intended audience has the hardware and the software capability to use the product. Pre-mastering of information for CDs may be acquired by the local command or agency separately from disc replication. Mastering and replication of the disc for command and agency publications should be acquired by the preparing agency.

a. Replication requirements for publications and forms. CDs containing authenticated departmental publications and forms should be submitted for replication as indicated below:

(1) For departmental (administrative) publications or forms, proponents submit a completed DA Form 260 to USAPPC for replication of CD containing

(a) only authenticated departmental (administrative) publications or forms or

(b) authenticated departmental (administrative) publications or forms that are combined with other products, such as multimedia products.

(2) For departmental training and doctrinal publications or forms, preparing agencies submit a completed DA Form 260 through TRADOC to USAPPC for replication of CD containing

(a) only authenticated departmental training and doctrinal publications or forms or

(b) authenticated departmental training and doctrinal publications or forms that are combined with other products, such as multimedia products.

(3) For departmental technical and equipment publications or forms, preparing agencies submit a completed DA Form 260 through AMC to USAPPC for replication of CD containing (a) only authenticated departmental technical and equipment publications or forms or (b) authenticated departmental technical and equipment publications or forms that are combined with other products, such as multimedia products.

(4) For other departmental publications, proponents submit a DA Form 260 to USAPPC for replication of CD containing

(a) only authenticated departmental (administrative) publications or forms or

(b) authenticated departmental (administrative) publications or forms that are combined with other products, such as multimedia products.

b. Stockage and distribution of CD: Stockage and distribution of CD products containing authenticated departmental publications should be accomplished through Army's standard DA Form 12-series distribution system. Initial distribution of CD products direct from the printer should be used where warranted.

c. Packaging requirements for publications: For CD containing only authenticated departmental publications regardless of the publication series or combination of series, the authentication block should also be displayed on the jewel box insert or mailer. For CD containing a combination of departmental and command publications, the authentication block of the appropriate departmental official should only be included on the departmental publication itself. The authentication block for departmental and command and agency publication compilations cannot be displayed on the jewel box insert or cardboard mailer, or face of the CD. If the jewel box packaging is proposed, the proponent justifies the request on DA Form 260.

d. Submission of DA Form 260, Request for Printing. Proponents must submit a completed DA Form 260 to USAPPC 30 days in advance of the required publication date of the CD. This allows time for indexing the CD product in DA Pamphlet 25-30.

e. Seals or emblems. For CDs that contain departmental publications, the label should not contain DOD, Army, or local command or agency seals or emblems.

f. Camera-ready art. Camera-ready art work submitted for discs, inserts, and packaging should meet the same standards of reproducibility as required for other departmental products. For any questions about color separation, registration, typography, or design, contact USAPPC, Typography and Design Branch at DSN 328-6268 or commercial at (703) 325-6268.

Glossary

Section I
Abbreviations

ACP	Allied Communications Publication
API	Application Program Interface
ASCII	American standard code for information interchange
ASD	Assistant Secretary of Defense
CALLCOMS	Center for Army Lessons Learned Collection and Observation Management System
C3I	command, control, communications, and intelligence
CFR	Code of Federal Regulations
COTS	Commercial off the Shelf
DBMS	Database Management System
DMS	Defense Message System
DOD	Department of Defense
FIPS	Federal Information Processing Standard
FOIA	Freedom of Information Act
FR	Federal Regulation
gif	Graphics Interchange Format
GILS	Government Information Locator Service
GRS	general records schedules
HTML	Hypertext Markup Language
ISO	International Standardization Organization
IT	Information Technology
LAN	Local Area Network
MHS	Mail Handling System or Message Handling System
NARA	National Archives and Records Administration
OCR	optical character reader
ODASD	Office of the Deputy Assistant Secretary of Defense
PDF	Portable Document Format
RFP	request for proposal
RMA	Records Management Application
SMTP	Simple Mail Transfer Protocol
SOW	statement of work
SQL	Structured Query Language
std	standard
TATSS	TRADOC Automated Training Scheduling System
TCP/IP	Transmission Control Protocol/Internet Protocol
TIFF	Tagged Image File Format
URI	Uniform Resource Indicator
URL	Uniform Resource Locator
URN	Uniform Resource Name
WAN	Wide Area Network

Section II
Terms

Abstract
A GILS data element that presents a narrative description of the information resource. This narrative should provide enough general information to allow the user to determine if the information resource has sufficient potential to warrant contacting the provider for further information.

Access constraints
This GILS data element is a grouping of subelements that together describe constraints or legal prerequisites for accessing the information resource or its component products or services. It includes General Access Constraints which subelement includes access constraints or legal prerequisites applied to assure the protection of privacy, and other special restrictions or limitations on obtaining the information resource.

Addressee
The name of the organization or individual to whom a record is addressed.

American Standard Code for Information Interchange (ASCII)
ASCII is a standard code for representing characters as binary numbers, used on most microcomputers, computer terminals, and printers. In addition to printable characters, the ASCII code includes control characters to indicate carriage return, backspace, etc.

Application Program Interface (API)
The API is defined as the interface between two software applications or between a software application and its platform which provide operating system services, network communication services, user interface services, data management services, and data interchange services.

Association
A relationship between or among records. Record associations include attachment and file.

Attachment
A record is associated with another record as an attachment when it is attached to the record and filed or transmitted between two persons.

Authentic record
A record that can be proven to be genuine based on its mode (i.e., method by which a record is communicated over space or time), form (i.e., format/media that a record has when it is received), state of transmission (i.e., the primitiveness completeness, and effectiveness of a record when it is initially set aside after being made or received), and manner of preservation and custody.

Authorized individual
A Records Manager and/or other persons specifically designated by the Records Manager as responsible for managing various aspects of an organization's records.

Author or originator
The author of a document is the physical person or the office/position responsible for the creation of the document. The author is usually indicted by the letterhead and/or signature. For RMS purposes the author/originator must be a personal name or official title, not a code or alias.

Case file
A folder or other file unit containing various information relating to a specific action, transaction, event, person, place, project, or other subject. A case file may cover one or many subjects that relate to the case. For example, a contract file contains records on a specific contract, such as applications, correspondence, addenda, reports, and processing documents. Other types of case files include official personnel folders, medical records, surveys, and studies.

Category code
A unique identifier assigned to a record group based on a file plan.

Control number
A GILS data element that is used to distinguish a locator record from all other GILS Core locator records. The control number should be distinguished with the record source agency acronym as provided in the U.S. Government Manual.

Controlled vocabulary
A GILS data element that is a grouping of descriptive terms that describe the resource and aids users in locating entries of potential interest.

Cross-reference
A GILS data element that is a grouping of subelements that together identify another locator record likely to be of interest. It is a listing of related information resources.

Cutoff
The termination or closing of files to permit their retirement, transfer, or destruction. After cutoff, no new records may be added to the file, nothing may be deleted or amended. Termination may be at regular intervals or conditional upon the occurrence of an event or condition. After a file is closed, a new file is established for records filed under the same subject or case.

Database
A database is a set of data consisting of at least one data file sufficient for a given purpose.

Database management system
A software system used to access and retrieve data stored in a database.

Data file
Related numeric, textual, or graphic information organized in a strictly prescribed form and format.

Date and time of creation
The data and time that the author/originator created the document. Date and time of creation must reflect the situation from the author/originator's point of view.

Date and time of receipt
The date and time of access by the addressee, not the date and time of delivery to the agency. If this data is provided by the computer system, it is required for documents that are received through electronic mail in a DOD agency.

Date and time of record
The date and time assigned by the computer at the time the record is filed in the RMA. A new version of the record must be filed separately with a new date and time. Version control arrangements link different versions of a record.

Date and time sent
The date and time that the message was sent or forwarded by the author. If this data is provided by the computer system, it is required for documents that are transmitted through electronic mail in a DOD agency.

Defense Message System (DMS)
The DMS is a Military Message Handling System (MMHS) based on ACP 123 for all military messages within the US. The DMS should support electronic mail, non-real time audio, video imagery, binary files, etc., in a store-and-forward messaging environment. The DMS embodies detailed guidance on national issues such as security, management, component implementation and policy as defined in the US Supplement-1, Update 2, to the ACP 123.

Digitization
The overarching term for the electronic recording of information via Internet (on-line-access), computer networks, computer disks (floppies, CD-ROMs), magnetic tapes, optical disks, satellite transmission, and bulletin boards. Digitization may be used for doctrine, training, leader development, organization, materials, and soldier (DTLOMS) purposes.

Digitized training
The digitization of training includes the development, implementation, distribution, and management of training primarily through electronic means. It provides the capability to train soldiers and units throughout the training environment.

Disposal
Actions taken regarding temporary (non-permanent) records when their retention period expires (destruction,

sale of paper records as waste, salvage of non-paper records, donation to eligible depository, erasure of electronic records).

Disposition code
An agency's alphanumeric or numeric code identifying the disposition instruction applicable to a record category.

Disposition instruction
A rule which specifies how long records in a record category must be kept to support the business need for which it was created, and states when it should be destroyed or transferred to the National Archives. Disposition instructions must be approved by the National Archives and Records Administration (NARA) and are mandatory. Authorized disposition instructions include those issued by NARA in a General Records Schedule (GRS) and those approved by NARA in response to a specific request. GRS instructions are applicable to all agencies of the Federal Government. Other authorized instructions are applicable in the requesting agency and any components identified by the agency in its request to NARA.

Distributor
A GILS data element that may include any of the following as well as locally defined elements: name, organization, street address, city, state, zip code, country, network address, hours of service, telephone, FAX.

Document
A document is information consigned to a medium. The traditional medium has been paper or other non-electronic medium. NOTE: In archival theory, all records are documents (they document something) but not all documents are records.

Electronic record
Electronic record means any information that is recorded in a form that requires a computer to process and satisfies the definition of a record in 36 CFR, Part 1234.

File
An aggregation of records, usually within a series, brought together because they relate to the same subject, activity or transaction. See Record Series.

File code
Record category code and extensions associated with a record indicating the specified arrangement in which it should be filed.

File plan
The records categorization scheme for an agency.

Format code
Codes indicating the logical structure of a record Graphics Interchange Format (gif) A compressed graphics file format used to upload, download, and store graphics sent via modem to and from on-line services. It is designed to minimize file transfer time over phone lines.

Government Information Locator Service (GILS)
GILS is a Federal Government service to help the general public locate and access information throughout the Federal Government. It describes the information available in those resources, and provides assistance in obtaining the information. GILS uses network technology and international standards for information search and retrieval. These standards are described in the Federal Information Processing Standard (FIPS) Publication 192, "Application Profile for the Government Information Locator Service."

Hypertext Mark Up Language (HTML)
A set of codes that form the standard of documents capable of being transported on the World Wide Web and read by a browser. The codes are used to identify the different parts of a document, specify the appearance of text and graphics, and form links between related topics. HTML is a subset of the Standard General Markup Language (SGML). HTML was originally developed at the CERN Institute in Switzerland and continues to undergo further development by a working group of the Internet Engineering Task Force.

Index terms
A GILS data element that is a grouping of descriptive terms drawn from a controlled vocabulary source to aid users in locating entries of potential interest.

Information
Facts or knowledge communicated or received.

Interoperability
Allows applications executing on separate hardware platforms, or in multi-processing environments on the same platform, to share data and cooperate in processing it through communications mechanisms such as remote procedure calls, transparent file access, etc.

Life cycle of records
The life cycle of records incorporates three stages: creation, maintenance and use, and disposition.

Linkage
A GILS terms used to describe the machine readable information used to encode resource location and identification information of electronic and other objects and to perform access (i.e., URI) to the resources. Examples include Uniform Resource Locators (URLs) and Uniform Resource Names (URNs).

Local subject index
A GILS data element that consists of a group of descriptive terms used to aid users in locating resources of potential interest, but the terms are not drawn from a formally registered controlled vocabulary source.

Media code
The code that represents the media of a record.

Media type
The material/environment on which information is inscribed (e.g., microform, electronic, paper).

Metadata
The values of the record profile attributes. See record profile.

Methodology
A GILS data element that identifies specialized tools, techniques, or methodology used to produce an information resource.

Non-record
Non-record materials are those that do not meet the definition of records (36 CFR, Part 1234). This includes materials that are not created or received under Federal Law or in connection with Government business; not preserved or considered appropriate for preservation because they lack evidence of agency or component activities or information of value. Non-record materials include extra copies of documents kept only for convenience of reference, stocks of publications and processed documents, and library or museum materials intended solely for reference or exhibit.

Office application
Software packages that perform a variety of office support functions, such as word processing, desktop, spreadsheet calculations, electronic mail, facsimile transmission and receipt, document imaging, optical character reader (OCR), work flow and data management. These applications are generally those used to generate, convert, transmit or receive business documents.

Order process
A GILS data element that provides information on how to obtain an information resource from a distributor.

Originating organization
Official name or code that reflects the office responsible for the creation of a document.

Organizational record
A record related to the tasks, functions, mission or operation of an organization. These records are divided into two subgroups, program and administrative records. Program records are those which relate to the mission and the specific functions for which an organization is responsible. Administrative records are those which relate to common support functions such as personnel, payroll, supply, station management, etc.

Portable Document Format (PDF)
PDF is a file format used to represent a document in a manner independent of the application software, hardware, and operating system used to create it.

Purpose
A GILS data element that describes why an information resource is offered and identifies other programs, projects, and legislative actions wholly or partially responsible for the establishment or continued delivery of the information resource. It may include the origin and lineage of the information resource and related information resources.

Record
Records include all books, papers, maps, photographs, machine-readable materials, and other documentary materials, regardless of physical form or characteristics, made or received by an office in connection with the transaction of official business and preserved or appropriate for preservation by that office as evidence of the organizations functions, policies, decisions, procedures, operations, or other activities of that office or because of the value of data in the record.

Record category
A level in a file plan; e.g., group, subgroup, series, file.

Record category status code
Code assigned to the values of this data element are used for event-driven disposition.

Record identifier
A sequentially-assigned, system-generated, unique number used to identify a particular record.

Record location
A pointer to the record. Examples: an operating system path-file name, the location of a file cabinet, the location of a magnetic tape rack.

Records management
The planning, controlling, directing, organizing, training, promoting, and other managerial activities involving the life cycle of records, including creation, maintenance (use, storage, retrieval) and disposition, regardless of media.

Records Management Application (RMA)
Software used by an organization to manage its records. Its primary management functions are: classifying and locating records, storing and retrieving records, and disposing of records.

Records manager
An individual responsible for the management of the records of an organization, IAW statutory and regulatory guidelines.

Record profile
Information (metadata) about a record that is used by the RMA to file and retrieve the record. It includes information fields such as to, from, date, subject, document type, format, location, record number, version number, file category, and originating organization. The data fields may also be used by the RMA as search criteria.

Record repository
A direct access device on which the electronic records and profiles are stored.

Record series
File units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, have a particular physical form, or for some relationship arising from their creation, receipt or use.

Record status action code
Code that indicates the action to be taken when a disposition date occurs (e.g., transfer or destroy).

Reliable records
Records that can be trusted due to their degree of completeness, the degree of control exercised on their creation and maintenance procedures, and/or the author's reliability.

Retention period
The length of time that records are to be kept prior to disposal or transfer to the National Archives.

Spatial reference
A GILS data element that provides the geographic areal domain of a data set or an information resource. The geographic names and coordinates can be used to define the bounds of coverage.

Subject
A principal topic addressed in a record.

Supplemental information
A GILS data element that is used to associate a record source with other descriptive information in the GILS core locator record.

Tagged-Image File Format
The Tagged-Image File Format (TIFF) is used to exchange documents between applications and computer platforms. The TIFF format supports LZW compression. LZW is the same compression used by the gif format; however, unlike gif, LZW TIFF supports image types other than indexed color.

Title
A GILS data element that is the distinguishing name of a document or documentary materials, such as films, sound recordings, images or graphics. The name may or may not be descriptive. In GILS terminology, the Title data element is used to convey the most significant aspects of the referenced resource and is intended for initial presentation to users independently of other elements. It should provide sufficient information to allow users to make an initial decision on likely relevance. It should convey the most significant information available, including the general topic area, as well as a specific reference to the subject.

Transmission data
Information in electronic message systems regarding the identities of sender and addressee(s), and the date and time messages were sent or received.

Use constraints
A GILS data element that describes constraints or legal prerequisites for using an information resource or its component, products, or services. This includes use constraints applied to assure the protection of privacy or intellectual property and other special restrictions or limitations on using the information resource.

Version
One of a sequence of documents having the same general form and specific subject and purpose. The sequence often reflects successive changes to a document.

Vital records
Records which contain information that is essential to the continued functioning or reconstitution of an organization to achieve its mission during and after an emergency. These records are essential to the protection of the rights and interests of that organization and of the individuals directly affected by its activities.

Vital record code
Code that indicates whether a record-category contains vital records.

X.400 Interpersonal Message System (IPMS)
International civilian standard for e-mail messaging - the P22 content type. This is the content type used in virtually all vendor supplied e-mail packages, that the primary content type used in e-mail communications on the Internet. Of the 93 Elements of Service in the P22 Content Type, only 21 are mandatory for support by all applications. Of the remaining 72 optional Elements of Service there is no requirement for vendors to implement them, though some are needed to satisfy DMS requirements. The result is that of the array of commercial products on the market that implement X.400 P22, full interoperability is largely non-existent. Implementation of content type P772 in the Defense Messaging System remedies this deficiency.

FOR THE COMMANDER:

OFFICIAL:

JAMES J. CRAVENS, JR.
Major General, GS
Chief of Staff

GARY E. BUSHOVER
Colonel, GS
Deputy Chief of Staff
for Information Management

DISTRIBUTION: H1; TRADOC Instl: D R1; S1